MONKSEATON HIGH SCHOOL

PRIVACY NOTICE
BIOMETRIC DATA

Status:

Statutory policy or document	Yes
Review frequency	3 yearly
Approval by	Governing Body
Approval date	7th February 2024

Publication:

Statutory requirement to publish on school website	Yes
Agreed to publish on school website	Yes

Review:

Frequency	Next Review Due
Every 3 years	February 2027

Version Control:

Author	Creation / Revision date	Version	Status
Business Manager (MAD)	January 2024	1.0	Final approved version for publication

Who is the Data Controller for the processing of Biometric Data?

Monkseaton High School is the Data Controller for any of the personal data processed by the school and this includes Biometric Data. This means we are responsible for making decisions about the data we collect, how we use it who we share it with, how long we keep it and why.

Cunninghams CRB is the data processor for the school's Biometric Data, this means that they only process data under specific written instruction from the school.

What is Biometric Data?
Biometric Data is special category personal information about an individual's physical or behavioural characteristics that can be used to identify that person. The Biometric Data used by the school is limited to facial scans of students and staff.

Why do you use Biometric Data and how does it work?
The school operates Cunningham's CRB system which allows students and staff to access school meals via a facial recognition scanner. By taking an image of you're a student's / member of staff's biometric data we can turn this information into a digital signature that can then be recognised by our systems. When the student is captured by the scanner at the till, the software matches their biometric image with the unique digital signature held in the database. Students and staff will then be able to purchase food and check account balances.

What does the law say about biometrics and school?
The Information Commissioner's Office considers all biometric information to be personal data as defined by the Data Protection Act 2018; this means that it must be obtained, used and stored in accordance with that act. We also comply with the requirements of the Protection of Freedoms Act 2012 whereby we notify each parent of our wish to use a biometric recognition system and seek consent to do so. In line with this act, should a student under the age of 18 refuse to participate in activities that involve the processing of their biometric data, we will ensure data is not taken. A student's objection or refusal, regardless of age, automatically overrides any parental consent to the processing of biometric data. The school will not process the biometric data of a student (under 18 years of age) where:

a) the child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;
b) no parent has consented in writing to the processing; or
c) one parent has objected in writing to such processing, even if another parent has given written consent.

Consent for the school to use biometric data can be withdrawn at any time. There will never be any circumstances in which the school will process a child's biometric information (for the purposes of using an automated biometric recognition system) without receiving appropriate consent.

What if we do not want to use the Biometeric system?
Where a refusal to the use of biometric data is made, we must legally provide an alternative solution for that student. Any student who does not wish to use or wishes to opt out of our biometric database will be able to use their name as an alternative.

Do you share Biometric Data with anybody else?
No, the software we use turns your child's biometric image in to a mathematical algorithm. The image of the biometric is then discarded. The information that is stored cannot be used to recreate an image of the child's biometric and we do not share it with anybody else.

What happens when a student leaves the School?
When a student leaves school all data relating to their biometric will be permanently deleted.

What happens to the face scan?
When a student registers to the biometric system, their face is scanned. The scan is then converted into a collection of data points via a mathematical algorithm. This data is then encrypted and stored on the student's account to be used as their unique identifier.

Are the face scans stored? No. The fingerprint is only used to generate a collection of data points which is then encrypted. The till reader looks for specific patterns and unique identifiers on the face, assigning specific data to each point - the face scan is never actually recorded.

Can the secure data be reversed to produce an image of the face?
No. The data points produced by the algorithm can't be reversed to produce an image of the face. The data is fully encrypted to military grade standards and even if this was to be broken, trying to reproduce an image if the face from the data points could never produce anything usable.

Is the Biometric Data secure? Our database is stored within the school on a secure server system. The database is fully password protected and cannot be accessed by the copying of the physical data files. The biometric data itself is encrypted within this database.